National Cybersecurity Center of Excellence

Mitigating IoT-Based DDoS

Industry Day

April 10, 2019

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Emergency Procedures for NCCoE Visitors

Evacuation Emergencies

What is an Evacuation Emergency?

- Fires
- Explosions
- Earthquakes
- Indoor toxic material releases
- Indoor radiological and biological accidents
- Workplace violence

What Will Happen During an Evacuation Event?

- A building-wide alarm will sound
- Verbal instructions over the building's public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest exit (Red Signs – **Upper Right Map**)
- If the Security Guard is close by and accessible, ask for further instruction
- Once outside the building, swiftly walk toward the designated meeting area near the posted sign stating "Evacuation Meeting Area" (Yellow Sign – **Lower Right Map**)

Shelter-In-Place (SIP) Emergencies

What is a Shelter-In-Place Emergency?

- Severe weather (hurricanes, tornadoes, etc.)
- chemical, biological, or radiological contaminants released into the environment

What Will Happen During an Evacuation Event?

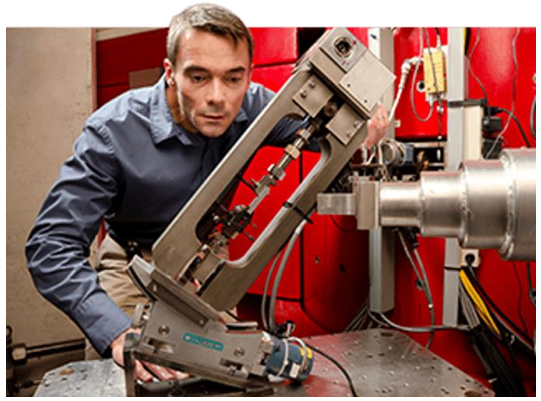
- A building-wide alarm will sound
- Verbal instructions over the building's public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest SIP hallway or room (Yellow Signs – **Upper Right Map**)
- If the Security Guard is close by and accessible, ask for further instruction

Agenda

9:00	Introduction to NCCoE and NIST IoT Program
9:10	Project Overview
9:25	MUD Specification Deep Dive
10:15	MUD at Morgan State University
10:30	Current State and Next Steps of the Project
10:45	Break
11:00	Build Demonstration Presentation
11:15	Panel Discussion
11:45	Optional Lab Tour

National Institute of Standards and Technology

National Institute of Standards and Technology



NIST is a bureau under the Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST runs a number of laboratories to assist in its mission.

Communications Technology Laboratory	Engineering Laboratory	Information Technology Laboratory	Material Measurement Laboratory	Physical Measurement Laboratory

NCCoE

NCCoE Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

Engagement and Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

Mitigating IoT-Based DDoS

Mitigating IoT-Based DDoS

Improving the security of home/consumer and small business IoT devices

Challenge

- IoT devices are given full connectivity to the internet by default
- Device security has not been a priority due to processing, timing, memory, and power constraints.
- Networked devices can be detected within minutes and exploited due to known security flaws, leading to easily scalable attacks.

Solution

- Security mechanisms that limit connectivity are emerging but adoption is lagging
- NCCoE is developing a proof of concept implementation levering current industry recommended standards and practices into the home or small business network to address security concerns.
- Automated method for reducing risk by implementing security mechanisms to provide frictionless methods to mitigate the attacks.

Project Purpose and Scope

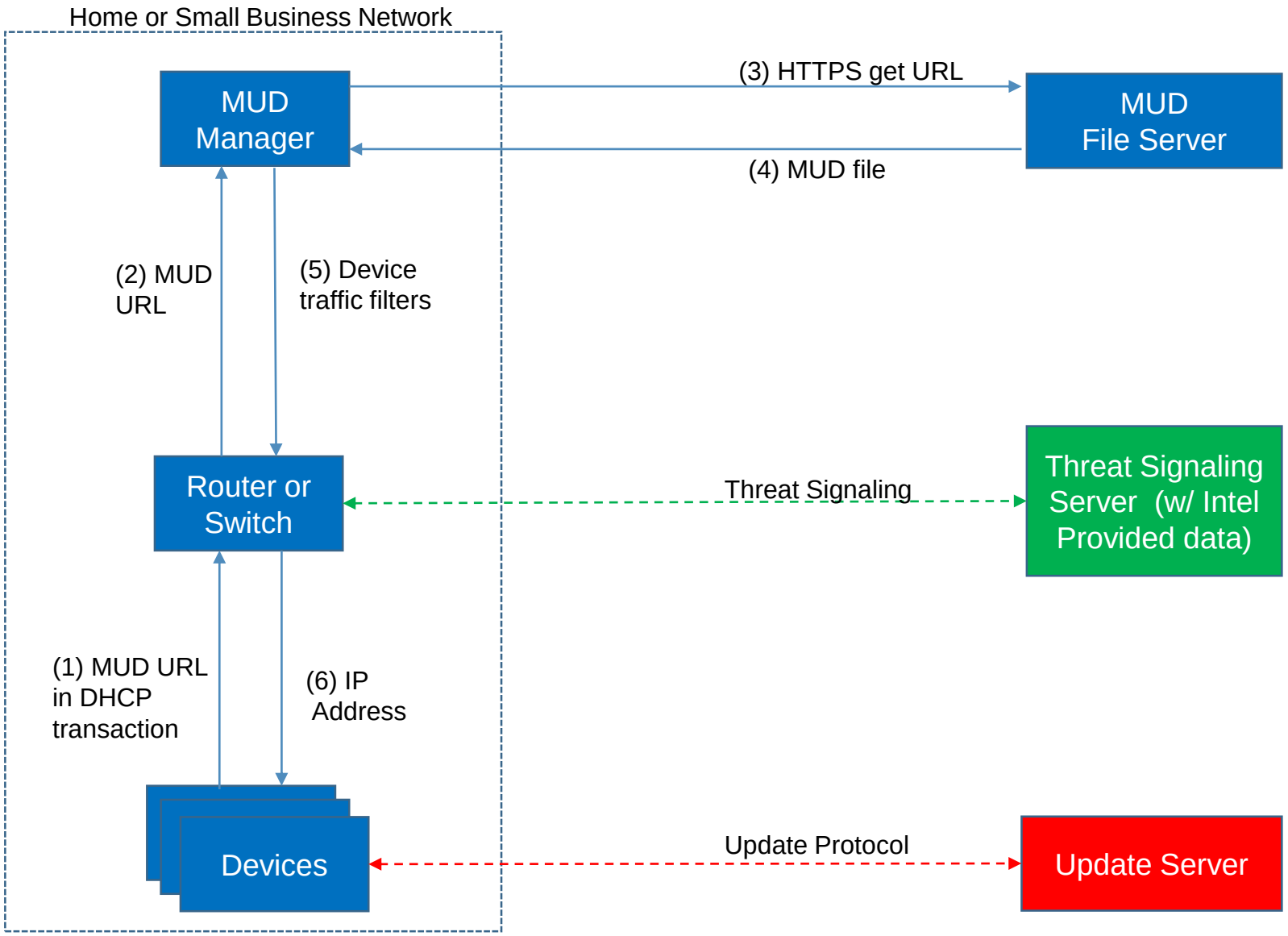
Purpose

- Reduce the vulnerability of IoT devices in home and business networks to botnets and other automated distributed threats, while limiting the utility of compromised IoT devices to malicious actors

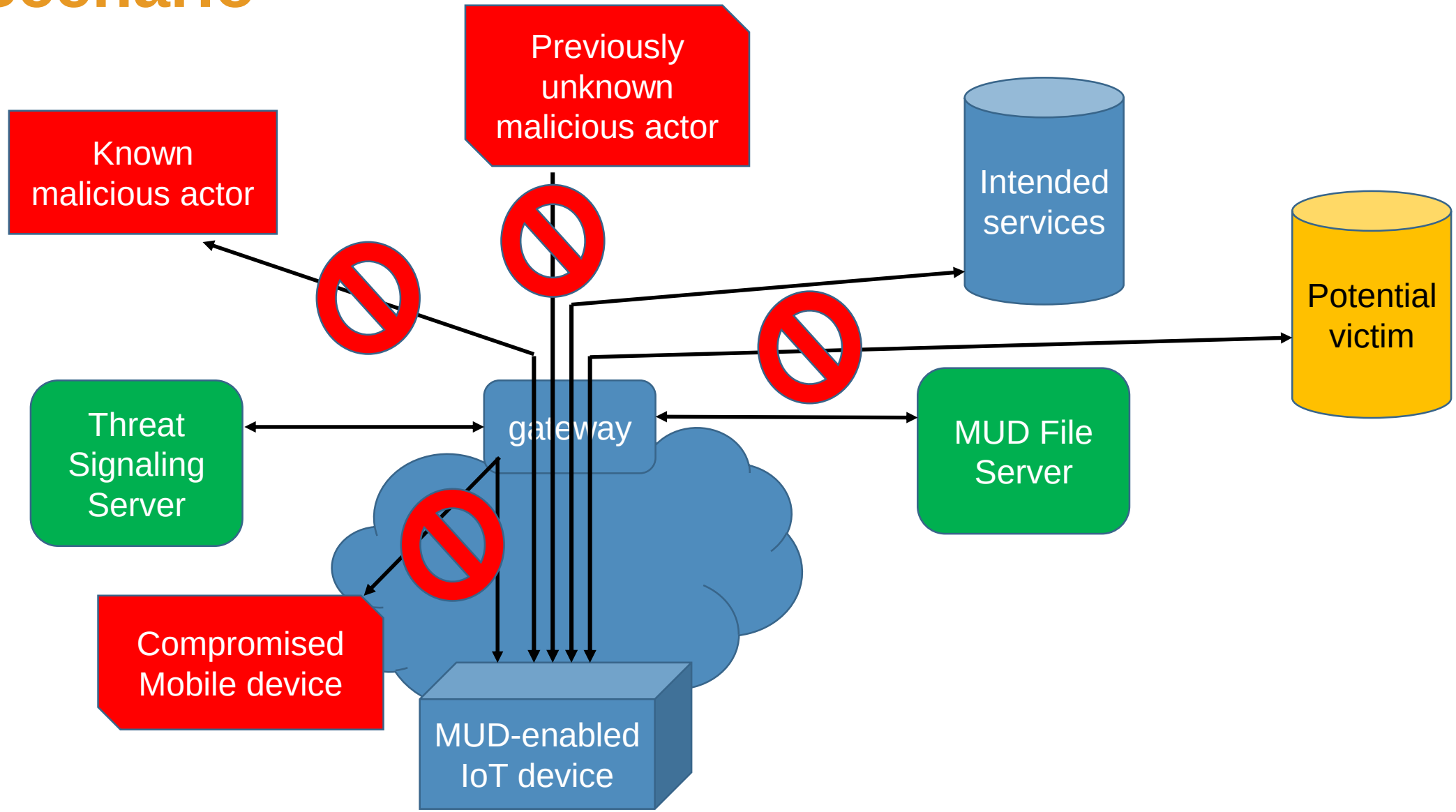
Scope

- Demonstrate a proposed approach for secured deployment of consumer and commercial IoT devices on home and small business networks
- Apply current and emerging network standards that are composed of both IoT and traditional devices in order to constrain communications-based malware exploits
- Network gateway components and security-aware IoT devices will leverage the Manufacturer Usage Description (MUD) Specification (RFC 8520)

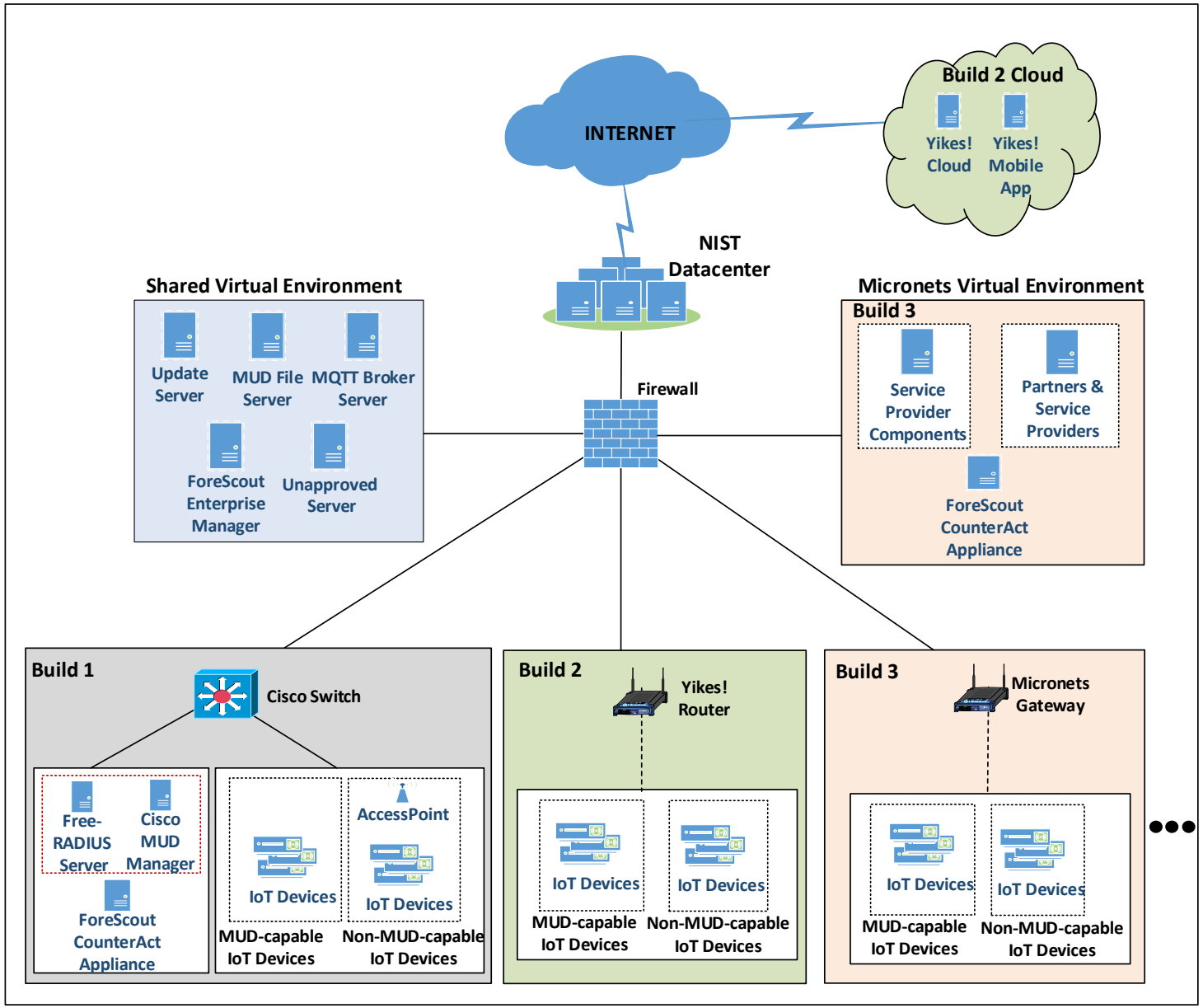
Logical Architecture



Scenario


Previously unknown malicious actor
Known malicious actor
Intended services
Potential victim
Threat Signaling Server
gateway
MUD File Server
Compromised Mobile device
MUD-enabled IoT device

Lab Architecture



Mitigating IoT-Based DDoS Collaborators